Remarks

The present amendment replies to an Office Action dated November 1, 2006. Claims 1, 2, and 4-40 are currently pending in the present application. Claims 1, 2, 4-9, and 40 have been withdrawn. In the Office Action, the Examiner rejected claims 10-39 on various grounds. The Applicants respond to each ground of rejection as subsequently recited herein and respectfully request reconsideration and further examination of the present application.

Information Disclosure Statement

The Examiner was not able to consider the document 389016 to Lin as the Examiner was unable to find a US patent document with that number. A Supplemental Information Disclosure Statement has been filed herewith correcting the Lin document to Taiwanese Patent No. 389016. The Lin document can be found on-line at www.delphion.com/details?pn=TW00389016B_ and at www.tipo.gov.tw/eng/howto/patdetail.asp?pn=389016&filingno=087117561. Copies of these web pages are attached.

35 U.S.C. §101

A. Claims 13-15, 21-22, 27-28, and 34-36 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Claims 13-15, 21-22, 27-28, and 34-36 are written in means-plus-function language, and so cover "the corresponding structure, material, or acts described in the specification and equivalents thereof." *See* 35 U.S.C. 112, sixth paragraph. The claims must be interpreted in light of the structure disclosed in the specification. *See* MPEP 2181. At least, Figures 1A, 1B, and 2 of the present Application disclose statutory subject matter for the means recited in the claims.

Withdrawal of the rejection of claims 13-15, 21-22, 27-28, and 34-36 under 35 U.S.C. §101 is respectfully requested.

35 U.S.C. §103

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references when combined must teach or suggest all the claim limitations. *See* MPEP 2143. The Applicants submit that the cited references fail to teach or suggest all the claim limitations and lack a suggestion or motivation to combine.

B. Claims 10, 13, and 16 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to Arnold (the *Arnold* patent) in view of U.S. Patent No. 6,748,530 to Aoki (the *Aoki* patent).

The *Arnold* patent and the *Aoki* patent, alone or in combination, fail to disclose, teach or suggest:

as to independent claim 10, a method for secure communication between a client and a server in a data processing system including an embedded client private key being associated with a client public key stored exclusively outside the client;

as to independent claim 13, an apparatus for secure communication between a client and a server in a data processing system including means for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded client private key being associated with a client public key stored exclusively outside the client; or

as to independent claim 16, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded client private key being associated with a client public key stored exclusively outside the client.

As admitted by the Examiner, the *Arnold* patent does not disclose **the embedded client private key being associated with a client public key stored exclusively outside the client**. The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. *See* column 4, lines 11-27.

The *Aoki* patent also fails to disclose this element and requires that **an individual public key be present at the client for at least part of the certification method, thus storing the individual public key in the client**. The Examiner asserts that the client does not store the client's public key and concludes that the client's public key is stored exclusively outside the client. The *Aoki* patent actually discloses that the individual public key is created and present at the client during individual temporary registration. *See* Figure 23; column 15, lines 58-64. A group public key is created and present at the client when creating the initial group. *See* Figure 25; column 16, lines 25-30. In addition, the individual public key of the responsible person is required for the encryption of the group private key when adding the responsible person private key to the group. *See* column 12, line 65 through column 13, line 1. The *Aoki* patent is silent as to whether the client retains or disposes of the public keys after use.

As acknowledged by the Examiner in the Examiner Interview Summary Record of April 10, 2006, the search of the prior art revealed that much of the prior art was silent on whether the client retained a copy of its public key. The Applicants' specification was amended to make it clear that the embedded client private key being associated with a client public key is stored exclusively outside the client.

The *Arnold* patent also lacks some suggestion or motivation to modify its teachings to embed a client private key in read-only memory. The *Arnold* patent discloses programming an MKS public signature key into the ROM of each secure chip to provide reliable access to the MKS public signature key. *See* column 4, lines 14-17. The MKS public signature key is used for authentication of messages received. The embedding of a client private key in read-only memory of the Applicants' invention serves a different function, i.e., to assure privacy of messages sent. Therefore, the *Arnold* patent lacks motivation to modify its teachings to provide the element as claimed.

The *Arnold* patent and the *Aoki* patent, alone or in combination, also lack a suggestion or motivation to combine the reference teachings. The *Arnold* patent is directed toward establishing a secure cryptographic network among operational units in a system. The *Aoki* patent is directed toward establishing a certification system for an entire enterprise. There is no need for the secure cryptographic network of the *Arnold* patent on top of the certification system of the *Aoki* patent, because the certification system is already secure.

Withdrawal of the rejection of claims 10, 13, and 16 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent is respectfully requested.

C. Claims 11, 14, and 17 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of U.S. Patent Publication No. US 2002/0078344 to Sandhu, *et al.* (the *Sandhu* publication).

As discussed in Section B above, the *Arnold* patent and the *Aoki* patent fail to disclose, teach, or suggest a client public key stored exclusively outside the client as recited in

independent claims 10, 13, or 16. The *Sandhu* publication also fails to disclose this element. The *Arnold* patent and the *Aoki* patent also lack a suggestion or motivation to modify or combine their teachings.

Claims 11, 14, and 17 depend directly from independent claims 10, 13, and 16, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Aoki* patents and the *Sandhu* publication, alone or in combination, fail to disclose a client public key stored exclusively outside the client. Therefore, the *Arnold* and *Aoki* patents and the *Sandhu* publication fail to disclose all the limitations of the rejected claims. The Applicants submit that claims 11, 14, and 17 are allowable for at least the reasons discussed above for their respective independent claims.

Withdrawal of the rejection of claims 11, 14, and 17 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication is respectfully requested.

D. Claims 12, 15, 18, 25, 27, 29, 26, 28, and 30 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication and further in view of U.S. Patent No. 5,970,147 to Davis (the *Davis* patent).

Regarding independent claims 10, 13, or 16, the *Arnold* patent and the *Aoki* patent fail to disclose, teach, or suggest a client public key stored exclusively outside the client as recited in independent claims 10, 13, or 16 as discussed in Section B above. The *Sandhu* publication also fails to disclose this element, as does the *Davis* patent. The *Arnold* patent and the *Aoki* patent also lack a suggestion or motivation to modify or combine their teachings.

Claims 12, 15, and 18 depend indirectly from independent claims 10, 13, and 16, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent, alone or in combination, fail to disclose a client public key stored exclusively outside the client. Therefore, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the

Davis patent fail to disclose all the limitations of the rejected claims. The Applicants submit that claims 11, 14, and 18 are allowable for at least the reasons discussed above for their respective independent claims.

Withdrawal of the rejection of claims 11, 14, and 18 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication and further in view of the *Davis* patent is respectfully requested.

Regarding claims 25, 27, 29, 26, 28, and 30, the *Arnold* patent, the *Aoki* patent, the *Sandhu* publication, and the *Davis* patent, alone or in combination, fail to disclose, teach, or suggest:

as to independent claim 25, a method for secure communication between a client and a server in a data processing system including retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client;

as to independent claim 27, an apparatus for secure communication between a client and a server in a data processing system including means for retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client; or

as to independent claim 29, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds

to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client.

As admitted by the Examiner, the *Arnold* patent does not disclose **the embedded client private key being associated with a client public key stored exclusively outside the client**. The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. *See* column 4, lines 11-27.

The *Aoki* patent also fails to disclose this element and requires that **an individual public key be present at the client for at least part of the certification method, thus storing the individual public key in the client.** The Examiner asserts that the client does not store the client's public key and concludes that the client's public key is stored exclusively outside the client. The *Aoki* patent actually discloses that the individual public key is created and present at the client during individual temporary registration. *See* Figure 23; column 15, lines 58-64. A group public key is created and present at the client when creating the initial group. *See* Figure 25; column 16, lines 25-30. In addition, the individual public key of the responsible person is required for the encryption of the group private key when adding the responsible person private key to the group. *See* column 12, line 65 through column 13, line 1. The *Aoki* patent is silent as to whether the client retains or disposes of the public keys after use. As acknowledged by the Examiner in the Examiner Interview Summary Record of April 10, 2006, the search of the prior art revealed that much of the prior art was silent on whether the client retained a copy of its public key. The Applicants' specification was amended to make it clear that the client public key is stored exclusively outside the client.

The *Sandhu* publication also fails to disclose a client public key stored exclusively outside the client, as does the *Davis* patent.

The *Arnold* patent also lacks some suggestion or motivation to modify its teachings to embed a client private key in read-only memory. The *Arnold* patent discloses programming an MKS public signature key into the ROM of each secure chip to provide reliable access to the MKS public signature key. *See* column 4, lines 14-17. The MKS public signature key is used for authentication of messages received. The embedding of a client private key in read-only memory of the Applicants' invention serves a different function, i.e., to assure privacy of messages sent. Therefore, the *Arnold* patent lacks motivation to modify its teachings to provide the element as claimed.

The *Arnold* patent and the *Aoki* patent, alone or in combination, also lack a suggestion or motivation to combine the reference teachings. The *Arnold* patent is directed toward establishing a secure cryptographic network among operational units in a system. The *Aoki* patent is directed toward establishing a certification system for an entire enterprise. There is no need for the secure cryptographic network of the *Arnold* patent on top of the certification system of the *Aoki* patent, because the certification system is already secure.

Claims 26, 28, and 30 depend directly from independent claims 25, 27, and 29, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent, alone or in combination, fail to disclose a client public key stored exclusively outside the client. Therefore, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent fail to disclose all the limitations of the rejected claims. The Applicants submit that claims 26, 28, and 30 are allowable for at least the reasons discussed above for their respective independent claims.

Withdrawal of the rejection of claims 25, 27, 29, 26, 28, and 30 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in

view of the *Sandhu* publication and further in view of the *Davis* patent is respectfully requested.

E. Claims 19, 21, 23, 31, 34, and 37 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of Examiner's Official Notice and further in view of the *Aoki* patent.

The *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice, alone or in combination, fail to disclose, teach, or suggest:

as to independent claim 19, a method for secure communication between a client and a server in a data processing system including retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client;

as to independent claim 21, an apparatus for secure communication between a client and a server in a data processing system including means for retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client;

as to independent claim 23, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client;

as to independent claim 31, a method for secure communication between a client and a server in a data processing system including retrieving an embedded client private key

from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key stored exclusively outside the client;

as to independent claim 34, an apparatus for secure communication between a client and a server in a data processing system including means for retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key stored exclusively outside the client; or

as to independent claim 37, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key stored exclusively outside the client.

As admitted by the Examiner, the *Arnold* patent does not disclose **the embedded client private key being associated with a client public key stored exclusively outside the client**. The *Arnold* patent diseloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. *See* column 4, lines 11-27.

The *Aoki* patent also fails to disclose this element and requires that **an individual public key be present at the client for at least part of the certification method, thus storing the individual public key in the client**. The Examiner asserts that the client does not store the client's public key and concludes that the client's public key is stored exclusively outside the client. The *Aoki* patent actually discloses that the individual public key is created and present at the client during individual temporary registration. *See* Figure 23; column 15, lines 58-64. A group public key is created and present at the client when creating the initial group. *See* Figure 25; column 16, lines 25-30. In addition, the individual public key of the responsible person is required for the encryption of the group private key when adding the responsible person private key to the group. *See* column 12, line 65 through column 13, line 1. The *Aoki* patent is silent as to whether the client retains or disposes of the public keys after use. As acknowledged by the Examiner in the Examiner Interview Summary Record of April 10, 2006, the search of the prior art revealed that much of the prior art was silent on whether the client retained a copy of its public key. The Applicants' specification was amended to make it clear that the client public key is stored exclusively outside the client.

The *Arnold* patent also lacks some suggestion or motivation to modify its teachings to embed a client private key in read-only memory. The *Arnold* patent discloses programming an MKS public signature key into the ROM of each secure chip to provide reliable access to the MKS public signature key. *See* column 4, lines 14-17. The MKS public signature key is used for authentication of messages received. The embedding of a client private key in read-only memory of the Applicants' invention serves a different function, i.e., to assure privacy of messages sent. Therefore, the *Arnold* patent lacks motivation to modify its teachings to provide the element as claimed.

The *Arnold* patent and the *Aoki* patent, alone or in combination, also lack a suggestion or motivation to combine the reference teachings. The *Arnold* patent is directed toward establishing a secure cryptographic network among operational units in a system. The *Aoki* patent is directed toward establishing a certification system for an entire enterprise. There is

no need for the secure cryptographic network of the *Arnold* patent on top of the certification system of the *Aoki* patent, because the certification system is already secure.

Withdrawal of the rejection of claims 19, 21, 23, 31, 34, and 37 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of Examiner's Official Notice and further in view of the *Aoki* patent is respectfully requested.

F. Claims 20, 22, 24, 32, 35, 38, 33, 36, and 39 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of Examiner's Official Notice and further in view of the *Aoki* patent and further in view of the *Sandhu* publication.

As discussed in Section E above, the *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice fail to disclose, teach, or suggest the client public key being stored exclusively outside the client as recited in independent claims 19, 21, or 23; or the embedded client private key being associated with a client public key stored exclusively outside the client, as recited in independent claims 31, 34, or 37. The *Sandhu* publication also fails to disclose this element. The *Arnold* patent and the *Aoki* patent also lack a suggestion or motivation to modify or combine their teachings.

Claims 20, 22, and 24 depend directly from independent claims 19, 21, and 23, respectively. Claims 32 and 33, claims 35 and 36, and claims 38 and 39 depend directly or indirectly from independent claims 31, 34, and 37, respectively. The dependent claims include all the elements and limitations of their respective independent claims. As discussed above, *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice, alone or in combination, fail to disclose a client public key stored exclusively outside the client. Therefore, *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice fail to disclose all the limitations of the rejected claims. The Applicants submit that claims 20, 22, 24, 32, 35, 38, 33, 36, and 39 are allowable for at least the reasons discussed above for their respective independent claims.

Withdrawal of the rejection of claims 20, 22, 24, 32, 35, 38, 33, 36, and 39 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the Examiner's Official Notice and further in view of the *Aoki* patent is respectfully requested.

Summary

Reconsideration of claims 10-39 is respectfully requested in light of the remarks herein. The Applicants submit that claims 10-39 as set forth by this Amendment fully satisfy the requirements of 35 U.S.C. §§ 102, 103, and 112. In view of foregoing remarks, favorable consideration and early passage to issue of the present application are respectfully requested.

Dated: February 1, 2007

Respectfully submitted,
David J. Craft, et al

/FRANK C. NICHOLAS/

CARDINAL LAW GROUP
1603 Orrington Avenue, Suite 2000
Evanston, IL 60201
(847) 905-7111

Frank C. Nicholas
Registration No. (33,983)
Attorney for Applicants